Math. & Sci. hum. / Mathematics and Social Sciences (46e année, n° 184, *2008*(4), p. 9–23)

CARACTÉRISATION DES QUENINES ET LEUR REPRÉSENTATION SPIRALE

Jean-Guillaume DUMAS[1]

RÉSUMÉ – *Les nombres de Raymond Queneau sont les entiers* n *pour lesquels la quenine (permutation spirale envoyant tout nombre pair sur sa moitié et tout nombre impair sur son opposé ajouté à* n*) est d'ordre maximal* n*. Nous étudions dans cette note la caractérisation des nombres de Queneau, les précédentes caractérisations étant à notre connaissance incomplètes. Nous proposons en outre une nouvelle représentation graphique, sous forme de spirale, à la fois des quenines à racine primitive différente de 2 et également des spinines, généralisation des quenines par la méthode des effacements de Jacques Roubaud. Nous étendons ensuite cette représentation spirale aux pérecquines.*

MOTS CLÉS – Pérecquine, Permutation de Queneau-Daniel, Quenine, Racine primitive, Spirale.

SUMMARY – Characterization of Quenines and their spiral representation
The Raymond Queneau numbers are the integers n *for which the quenine (the spiral permutation sending even numbers to their halves and odd numbers to their opposites added to* n*) is of order* n*. In this note, we study the characterization of Queneau numbers, since previous characterizations one, to our knowledge incomplete. We also propose a new graphical representation, of spiral shape, both of the quenines with primitive root distinct from 2 and of the spinines, which generalize quenines by Jacques Roubaud's erasing technique. We then extend this representation to pérecquines.*

KEYWORDS – Perecquine, Primitive root, Queneau-Daniel permutation, Quenine, Sestina, Spiral.

1. L'OULIPO, LA POÉSIE DES TROUBADOURS ET LES QUENINES

Arnaut Daniel est un troubadour de la fin du XIIe siècle. Un de ses poèmes célèbres, *ongle et oncle* (cf. Figure 1), est une série de six strophes de six vers chacune [Roubaud, 1969]. Chacun des mots à la rime de la première strophe est reproduit dans les strophes suivantes dans un autre ordre. Plus précisément, chaque passage d'une strophe à l'autre est déterminé de la même façon, à l'aide de la spirale de la Figure 2 :

[1]Laboratoire J. Kuntzmann, 51, rue des Mathématiques, Université de Grenoble, UMR CNRS 5224, BP 53X, 38041 Grenoble, Jean-Guillaume.Dumas@imag.fr

Sextine

Ce vœu dur qui dans le cœur m'entre,
nul bec ne peut le déchirer, ni ongle
de lausengier, qui médisant perd l'âme ;
et ne l'osant battre à branche ou à verge,
secrètement, là où il n'y a point d'oncle,
j'aurai ma joie en verger ou en chambre.

Quand j'ai souvenir de la chambre
où à mon dam je sais que pas un n'entre,
tant me sont durs plus que frère ni oncle
nul membre n'ai qui ne tremble, ni d'ongle,
plus que ne fait l'enfant devant la verge :
telle est ma peur de l'avoir trop dans l'âme !

Puisse-t-elle de corps, non d'âme,
me recevoir en secret dans sa chambre !
Car plus me blesse au cœur que coup de verge
si qui la sert là où elle est ne rentre !
Toujours serai pour elle chair et ongle
et ne croirai conseil d'ami ni d'oncle.

Et jamais la sur de mon oncle
je n'aimai plus ni tant, de par mon âme
Et si voisin que l'est le doigt de l'ongle,
je voudrais être, à son gré, de sa chambre
plus peut L'Amour qui dans le cœur me rentre
faire de moi qu'un fort de frêle verge.

Car depuis que fleurit la verge
sèche et qu'Adam légua neveux et oncles,
si fine amour, qui dans le cœur me rentre,
ne fut jamais en corps, ni même en âme ;
où qu'elle soit, dehors ou dans sa chambre,
mon cœur y tient comme la chair à l'ongle.

Car ainsi se prend et s'énongle
mon cœur en elle ainsi qu'écorce en verge ;
elle est de joie tour et palais et chambre,
et je ne prise autant parents ni oncle :
au ciel j'aurai deux fois joyeuse l'âme,
si jamais nul, de trop aimer, n'y entre.

Arnaut envoie sa chanson d'ongle et d'oncle
à toi qui tiens son âme sous ta verge,
son Désiré, dont le prix en chambre entre.

Sestina

Lo ferm voler qu'el còr m'intra
no'm pùt ges bècs escoissendre ni ongla
de lausengièr, qui pèrd per mal dir s'arma ;
e car non l'aus batre amb ram ni amb verja,
sivals a frau, lai ont non aurai oncle,
jausirai jòi, en vergièr o dins chambra.

Quand mi soven de la chambra
ont a mon dam sai que nulhs òm non intra,
ans me son tuch plus que fraire ni oncle,
non ai membre no'm fremisca, neis l'ongla,
aissì com fai l'énfans denant la verja :
tal paor ai no'l sia tròp de l'arma.

Del còr li fos, non de l'arma,
e consentis m'a celat dins sa chambra !
Que plus mi nafra'l còr que còps de verja
car lo sieus sèrvs lai ont ilh es non intra ;
tots temps serai amb lièis com charns et ongla,
e non creirai chastic d'amic ni d'oncle.

Anc la seror de mon oncle
non amèi plus ni tant, per aquesta'arma !
Qu'aitant vesins com es lo dets de l'ongla,
s'a lièis plagués, vòlgra èsser de sa chambra ;
de mi pòt far l'amors qu'ins el còr m'intra
mièlhs a son vòl qu'òm fòrts de frévol verja.

Puèis florit la secha verja
ni d'En Adam mògron nebot ni oncle,
tant fina amors com cela qu'el còr m'intra
non cug fos anc en còrs, ni eis en arma ;
ont qu'ilh estei, fòrs en plaça o dins chambra,
mos còrs no's part de lièis tant com ten l'ongla.

Qu'aissi s'enpren e s'enongla
mons còrs en lièis com l'escòrça en la verja ;
qu'ilh m'es de jòi tors e palatz e chambra,
e non am tant fraire, parent ni oncle :
qu'en paradis n'aurà doble jòi m'arma,
si ja nulhs òm per ben amar lai intra.

Arnauts tramet sa chançon d'ongla e d'oncle,
a grat de lièis que de sa verja à l'arma,
son Desirat, cui prètz en chambra intra.

FIGURE 1. Ongle et oncle, Arnaut Daniel, XIIe siècle

	§1	σ_6	§2	§3	§4	§5	§6
$\mathcal{O}_6(1)$	1	$\rightarrow$	6	3	5	4	2
	2	$\rightarrow$	1	6	3	5	4
	3	$\rightarrow$	5	4	2	1	6
	4	$\rightarrow$	2	1	6	3	5
	5	$\rightarrow$	4	2	1	6	3
	6	$\rightarrow$	3	5	4	2	1

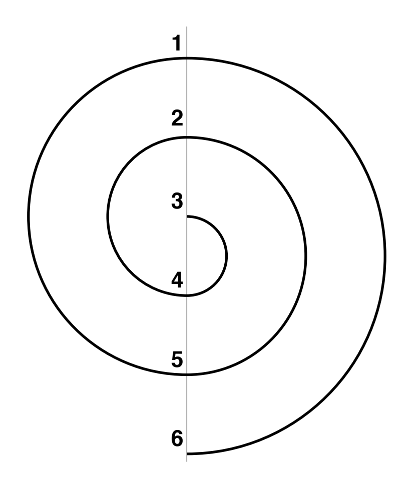


FIGURE 2. Permutation spirale de la sextine

En effet, si l'on inscrit de haut en bas les rimes d'une strophe, dans la strophe suivante, ces rimes se retrouvent dans l'ordre donné lorsque l'on suit les méandres de la spirale : en partant du bas, en 6, on tourne pour rencontrer successivement 1, 5, 2, 4, 3 qui forment bien les rimes de la deuxième strophe. Ce type de permutation sur 6 vers est appelé une sextine et a été généralisé à n vers par Raymond Queneau.

DÉFINITIONS 1 (Bringer, 1969).
- *Une* permutation spirale *est une permutation σ_n de l'ensemble* $\{1, 2, \ldots, n\}$ *vérifiant la condition suivante :*

$$\begin{aligned} \sigma_n(2p) &= p \\ \sigma_n(2p+1) &= n - p \end{aligned}$$

- *Le sous-groupe cyclique G_n, engendré par σ_n est le groupe de Queneau-Daniel.*
- *Les entiers n tels que G_n soit de cardinal n sont dits* admissibles.
- *Une permutation spirale avec n admissible est appelée une* quenine*, ou encore une n^{ine}.*

Autrement dit, n est admissible si et seulement si les *orbites poétiques* de chacune des rimes sont d'*ordre spiralique n*, i.e. chaque rime se trouve une seule fois à un endroit donné de la strophe dans l'ensemble du poème. Arnaut Daniel a exhibé une quenine de cardinal 6, mais toutes les quenines ne sont pas possibles : par exemple, il n'y a pas de quenine de cardinal 4, puisque, par exemple, l'orbite de 3 est le singleton $\{3\}$ [Roubaud, 1993]. L'Oulipo, et plus particulièrement Jacques Roubaud, s'est alors intéressé à la quête des quenines, à l'aide des corps finis.

En effet, considérons la permutation δ_n, inverse de σ_n. Celle-ci peut être définie comme suit [Audin, 2007] :

$$\delta_n(x) = \begin{cases} 2x & \text{si } 2x \leq n \\ 2n + 1 - 2x & \text{sinon} \end{cases}$$

DÉMONSTRATION. Soit x tel que $2x \leq n$ alors $\sigma_n \circ \delta_n(x) = \sigma_n(2x) = x$. Pour x tel que $2x > n$ alors $\sigma_n \circ \delta_n(x) = \sigma_n(2(n-x)+1) = n - (n-x) = x$. Donc $\sigma_n \circ \delta_n = Id$ et σ_n étant bijective, δ_n est son inverse. □

Il est clair que les cardinaux des sous-groupes cycliques engendrés par δ_n ou σ_n sont identiques. Il revient donc au même d'étudier l'un ou l'autre des sous-groupes. L'idée est de considérer les entiers modulo $2n+1$. Dans ce cas, $\delta_n(x)$ est simplement plus ou moins $2x$: il existe un $e \in \{0,1\}$ tel que $\delta_n(x) \equiv (-1)^e 2x[2n+1]$. À partir de là Monique Bringer a montré un certain nombre de résultats dont les suivants :

THÉORÈME 1 (Bringer, 1969).
- *Si n est admissible alors $2n+1$ est premier.*
- *$n = 4p$ n'est pas admissible.*
- *$n = 2^p - 1$ n'est pas admissible.*
- *Si n et $2n+1$ sont premiers, n est admissible.*
- *Si $n = 2p$ et que p et $4p+1 = 2n+1$ sont premiers, n est admissible.*

DÉMONSTRATION. Reprenons seulement de [Bringer, 1969] la preuve que $2n+1$ est forcément premier. Sinon, il existe q un diviseur de $2n+1$ avec $q > 1$. Dans ce cas, pour tout m de l'orbite de q, on a $m \equiv (-1)^e 2^k q$. Ce qui implique forcément que q divise m puisqu'il divise à la fois $2n+1$ et $(-1)^e 2^k q$. Donc l'orbite de q ne contient que des diviseurs de q. Or, $1, \ldots, q-1$ ne divisent pas q donc l'orbite de q ne peut être complète. Par la suite $2n+1$ ne peut être admissible. □

Or, il est possible de complètement caractériser les quenines. Ceci peut être fait avec un peu de théorie des corps finis.

2. CARACTÉRISATION DES QUENINES

Nous rappelons qu'un générateur du groupe des inversibles d'un corps fini est appelé une *racine primitive de l'unité*. En effet c'est une racine $q-1$-ième de 1 et la primitivité vient du fait qu'elle n'est pas une racine d'ordre inférieur.

Nous avons vu que Monique Bringer a donné une condition suffisante et les cas particuliers du Théorème 1 ; Jacques Roubaud donne une caractérisation dans [Roubaud, 1993, 2.4.II] qui semble incorrecte : « Une condition nécessaire et suffisante pour que n soit admissible est qu'il soit d'ordre n ou $2n$ dans le groupe multiplicatif des entiers modulo $2n+1$. »

Dans cette caractérisation, le cas où n est pair n'est pas considéré : un contre exemple simple est celui de l'octine : 2 est d'ordre 8 modulo 17, mais malheureusement l'orbite de 2 n'est que d'ordre spiralique 4, ce qui rend l'octine impossible.

Nous donnons donc ici une caractérisation complète :

THÉORÈME 2. *$2n+1$ étant premier, soit $\mathbb{Z}/_{2n+1}\mathbb{Z}$ le corps à $2n+1$ éléments, alors n est admissible si et seulement si :*
- *Soit 2 est d'ordre $2n$ (2 est racine primitive) dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.*
- *Soit n est impair et 2 est d'ordre n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.*

DÉMONSTRATION. Tout d'abord prouvons la condition nécessaire. Comme l'ordre de 2 divise $2n$, le cardinal des inversibles de $\mathbb{Z}/_{2n+1}\mathbb{Z}$, les seuls ordres possibles, différents de n et $2n$, sont strictement inférieurs à n. Supposons que 2 est d'ordre $j < n$. Alors nous avons $\delta_n^j(2) \equiv \pm 2^j 2 \equiv \pm 2$. Nous avons donc deux cas :

1. Si $\delta_n^j(2) = 2$, alors l'orbite de 2 ne contient que $j < n$ éléments, ce qui n'est pas suffisant car n est supposé admissible.
2. Dans l'autre cas, $\delta_n^j(2) \equiv -2$. Or $1 \leq \delta_n^j(x) \leq n$ par définition. Donc $1 \leq 2n+1-2 \leq n$, ou encore $n \leq 1$. Mais 2 est d'ordre 2 modulo $2*1+1 = 3$.

Donc si n est admissible, alors 2 est d'ordre n ou $2n$ modulo $2n+1$.

Il ne nous reste plus qu'à exclure le cas où $n = 2p$ est pair et 2 est d'ordre n modulo $2n+1$. En effet, dans ce cas $2^p \equiv -1$ $[2n+1]$. Il s'en suit que $\delta_n^p(2) \equiv (-1)^k 2^p 2 \equiv \pm 2$. Or, nous avons vu que $\delta_n^p(2) \neq -2$. Il s'en suit de nouveau que la seule possibilité est $\delta_n^p(2) \equiv 2$. Mais alors n n'est pas admissible puisque l'orbite de 2 par δ_n ne contient qu'au plus $p = \frac{n}{2} < n$ éléments distincts.

Nous prouvons ensuite la condition suffisante. Prenons ω le cardinal de la plus petite orbite des éléments de $\{1, \dots, n\}$ par δ_n et supposons que l'élément u soit d'ordre ω. Dans ce cas, le fait qu'il existe k tel que $\delta_n^\omega(u) \equiv u \equiv (-1)^k 2^\omega u$. implique donc que $(-1)^k 2^\omega \equiv 1$, car u est inversible. Cela revient à $2^\omega \equiv \pm 1$ et il y a deux cas :

1. Si $2^\omega \equiv 1$. Alors ω est plus grand que l'ordre de 2. Donc $\omega \geq n$ et donc $\omega = n$ car la permutation est au plus d'ordre n.
2. Si $2^\omega \equiv -1$ Alors
   (a) Soit l'ordre de 2 est $j = 2n$ et donc $2^n \equiv -1$. Ainsi $2^{n+\omega} = 1$ et donc $\omega = n$.
   (b) Soit l'ordre de 2 est $j = n$ et n est impair. Alors $(2^\omega)^2 = (-1)^2 = 1$, ce qui prouve que n divise 2ω. Or n est impair donc le lemme de Gauß implique que n divise ω. Là encore $\omega = n$.

□

Ainsi, nous pouvons décider facilement si une quenine donnée existe ou non. La Table 1 donne les 178 premières quenines[2].

1	2	3$^\diamond$	5	6	9	11$^\diamond$	14	18	23$^\diamond$	26	29	30	33
35$^\diamond$	39$^\diamond$	41	50	51$^\diamond$	53	65	69	74	81	83$^\diamond$	86	89	90
95$^\diamond$	98	99$^\diamond$	105	113	119$^\diamond$	131$^\diamond$	134	135$^\diamond$	146	155$^\diamond$	158	173	174
179$^\diamond$	183$^\diamond$	186	189	191$^\diamond$	194	209	210	221	230	231$^\diamond$	233	239$^\diamond$	243$^\diamond$
245	251$^\diamond$	254	261	270	273	278	281	293	299$^\diamond$	303$^\diamond$	306	309	323$^\diamond$
326	329	330	338	350	354	359$^\diamond$	371$^\diamond$	375$^\diamond$	378	386	393	398	410
411$^\diamond$	413	414	419$^\diamond$	426	429	431$^\diamond$	438	441	443$^\diamond$	453	470	473	483$^\diamond$
491$^\diamond$	495$^\diamond$	509	515$^\diamond$	519$^\diamond$	530	531$^\diamond$	543$^\diamond$	545	554	558	561	575$^\diamond$	585
593	606	611$^\diamond$	614	615$^\diamond$	618	629	638	639$^\diamond$	641	645	650	651$^\diamond$	653
659$^\diamond$	683$^\diamond$	686	690	713	719$^\diamond$	723$^\diamond$	725	726	741	743$^\diamond$	746	749	755$^\diamond$
761	765	771$^\diamond$	774	779$^\diamond$	783$^\diamond$	785	791$^\diamond$	803$^\diamond$	809	810	818	831$^\diamond$	833
834	846	866	870	873	879$^\diamond$	891$^\diamond$	893	911$^\diamond$	923$^\diamond$	930	933	935$^\diamond$	938
939$^\diamond$	950	953	965	974	975$^\diamond$	986	989	993	998				

TABLE 1. Les quenines inférieures à 1000. $^\diamond$ indique que 2 est d'ordre n dans $\mathbb{Z}/2n+1\mathbb{Z}$

[2] Dans [Roubaud, 1993], Jacques Roubaud indique que 141 est une quenine, ceci est inexact [Esposito, 2000] : en particulier, 2 est d'ordre seulement $94 = 2*47 < 141 = 3*47$ modulo 283.

Cette suite se retrouve sur le site de l'encyclopédie en ligne des suites d'entiers de N. J. A. Sloane à la référence $A054639$[3]. Il est à noter que Joerg Arndt a conjecturé la caractérisation suivante des quenines [Arndt, 2009, 41.8.2] : elles correspondent aux « bases normales optimales de type 2 dans $\mathtt{GF}(2^n)$ ». En fait cette conjecture est une conséquence directe du Théorème 2 et se réécrit de la manière suivante :

COROLLAIRE 1. *$2n+1$ étant premier, soit $\mathbb{Z}/_{2n+1}\mathbb{Z}$ le corps à $2n+1$ éléments, alors n est admissible si et seulement si :*
- *Soit 2 est d'ordre $2n$ dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$ et $n \equiv 1$ ou $2 \mod 4$.*
- *Soit 2 est d'ordre n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$ et $n \equiv 3 \mod 4$.*

DÉMONSTRATION. Les différences entre le corollaire et le Théorème 2 résident dans les deux points suivants :

1. 2 est d'ordre $2n$ est incompatible avec $n \equiv 3 \mod 4$.
2. 2 est d'ordre n est incompatible avec $n \equiv 1 \mod 4$.

Dans les deux cas le caractère de résiduïcité de 2 (voir par exemple [Bach, 1996, Théorème 5.8.1]) nous donne la réponse :

1. Si $n \equiv 3 \mod 4$ alors $2n+1 \equiv 7 \mod 8$ et donc 2 est un résidu quadratique modulo $2n+1$. Ce qui implique que l'ordre de 2 ne peut donc pas être maximal $2n$, mais seulement inférieur ou égal à n.
2. Au contraire, si $n \equiv 1 \mod 4$ alors $2n+1 \equiv 3 \mod 8$ et donc dans cas 2 n'est pas un résidu quadratique modulo $2n+1$. Supposons alors que l'ordre de 2 est n. Il s'en suit que $2^n \equiv 1$ ou encore $2^{4k+1} \equiv 1$. Cela implique que $2^{4k+2} \equiv \left(2^{2k+1}\right)^2 \equiv 2$ et donc 2 serait un résidu quadratique ce qui est absurde.

□

3. GÉNÉRALISATIONS DES QUENINES

Jacques Roubaud, dans [Roubaud, 1993] généralise les quenines aux k-quenines, permutations pour lesquelles la multiplication par 2 est remplacée par une multiplication par k, considérons $\delta_{3,n}(x)$:

$$\delta_{3,n}(x) = \begin{cases} 3x & \text{si } 3x \leq n \\ 2n+1-3x & \text{si } n < 3x \leq 2n \\ 3x-(2n+1) & \text{sinon} \end{cases}$$

Notons que $2n+1$ étant premier, $3x$ ne peut pas être égal à $2n+1$. Cette généralisation donne par exemple directement l'octine, ou 3-quenine : $1 \quad \rightarrow \quad 6 \;\; 2 \;\; 5 \;\; 4 \;\; 7 \;\; 8 \;\; 3$.

La Table 2 donne les entiers dont 3 est une racine primitive de $2n+1$, premier, qui ne sont pas des 2-quenines.

Dans le cas de 3, et plus généralement pour tout k, 3 est appelé le *multiplicateur* de la quenine et $\frac{n}{k}$ est appelé le *rayon*, pour la raison qui suit.

[3] http ://www.research.att.com/~njas/sequences/A054639.

8	15	21	44	56	63	68	111	116	125$^\diamond$	128	140	141
165	176	200	224	260	284	285	296	308	315	320	345	369
404	405	428	440	455$^\diamond$	464	476	485$^\diamond$	488	506	524	548	551$^\diamond$
581$^\diamond$	596	608	663	680	704	711	716	729	740	776	789	800
806	813	848	849	854	860	861	905$^\diamond$	915	944	956	999	

TABLE 2. Les 3-quenines inférieures à 1000 qui ne sont pas des 2-quenines. $^\diamond$ indique que 3 est d'ordre n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.

En effet, la représentation en spirale n'est plus valable, il faut l'adapter à la racine primitive 3, i.e. aux trois cas possibles dans la définition de σ ou δ. L'idée est de considérer 3 « rayons » comme sur les Figures 3 et 4.

Comme il est possible d'utiliser n'importe quelle racine primitive, il faut donc généraliser cette représentation à une spirale comportant un nombre de rayons exactement égal au multiplicateur (i.e. à la racine primitive utilisée).

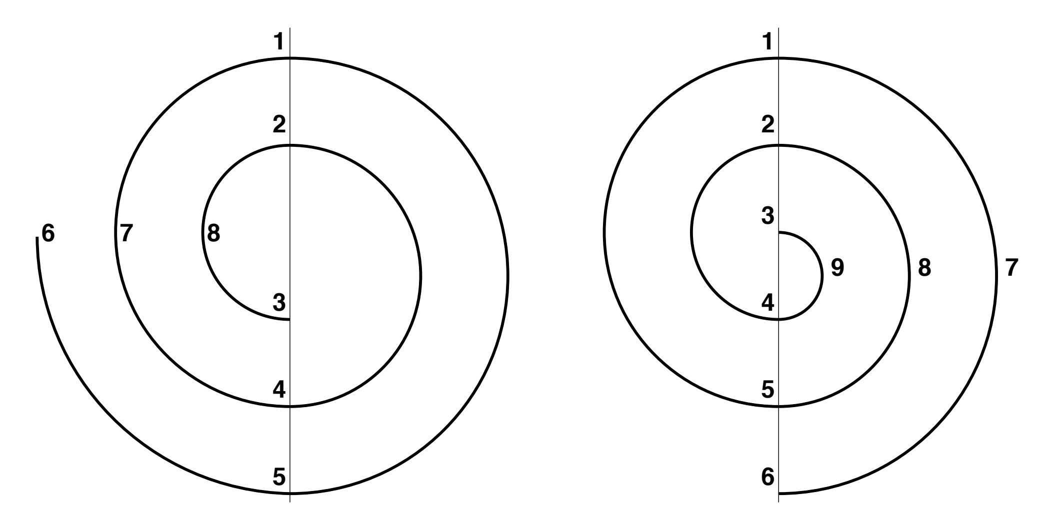


FIGURE 3. La 3-octine

FIGURE 4. La 3-neuvine

Ainsi, tous les entiers n dont $2n+1$ est premier permettent d'avoir une permutation spirale généralisée. Il suffit de savoir fabriquer des racines primitives. En particulier, la plus petite racine primitive est intéressante puisqu'elle permet d'avoir la représentation spirale la plus "simple" en ce sens qu'elle présente le moins de rayons possibles.

DÉFINITION 1. *La* plus petite racine primitive *de m est notée $\chi(m)$.*

4. CARACTÉRISATION GÉNÉRALE

Dans cette section, nous étendons la caractérisation du Théorème 2 à toutes les racines primitives, en notant $\delta_{n,g}$ la permutation spirale de multiplicateur g :

THÉORÈME 3. *Soit n un entier tel que $2n+1$ est premier et soit $g \leq n$. Soit $\mathbb{Z}/_{2n+1}\mathbb{Z}$ le corps à $2n+1$ éléments, alors $\delta_{n,g}$ est d'ordre n si et seulement si :*

- *Soit g est d'ordre $2n$ (g est racine primitive) dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.*
- *Soit n est impair et g est d'ordre n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.*

La preuve est identique à celle du Théorème 2 à l'exception de la condition $g \leq n$:

DÉMONSTRATION. Supposons que g est d'ordre $j < n$. Alors nous avons $\delta^j_{n,g}(g) \equiv \pm g^j g \equiv \pm g$. Nous avons donc deux cas :

1. Si $\delta^j_{n,g}(g) = g$, alors l'orbite de g ne contient que $j < n$ éléments, ce qui n'est pas suffisant car n est supposé admissible.
2. Dans l'autre cas, $\delta^j_{n,g}(g) \equiv -g$. Or $1 \leq \delta^j_{n,g}(x) \leq n$ par définition. Donc $1 \leq 2n+1-g \leq n$, ou encore $n < g$. C'est là que la condition supplémentaire est nécessaire.

Donc si n est admissible, alors g est d'ordre n ou $2n$ modulo $2n+1$.

Il ne nous reste plus qu'à exclure le cas où $n = 2p$ est pair et g est d'ordre n modulo $2n+1$. En effet, dans ce cas $g^p \equiv -1\ [2n+1]$. Il s'en suit que $\delta^p_{n,g}(g) \equiv (-1)^k g^p g \equiv \pm g$. Or, nous avons vu que $\delta^p_{n,g}(g) \neq -g$, grâce à la condition et par ailleurs, $\delta^p_{n,g}(g) \equiv g$ impliquerait que l'orbite de g ne contienne qu'au plus $p = \frac{n}{2} < n$ éléments.

Nous prouvons ensuite la condition suffisante. Prenons ω le cardinal de la plus petite orbite des éléments de $\{1, \ldots, n\}$ par $\delta_{n,g}$ et supposons que l'élément u soit d'ordre ω. Dans ce cas, le fait qu'il existe k tel que $\delta^\omega_{n,g}(u) \equiv u \equiv (-1)^k g^\omega u$. implique donc que $(-1)^k g^\omega \equiv 1$, car u est inversible. Cela revient à $g^\omega \equiv \pm 1$ et il y a deux cas :

1. Si $g^\omega \equiv 1$. Alors ω est plus grand que l'ordre de g. Donc $\omega \geq n$ et donc $\omega = n$ car la permutation est au plus d'ordre n.
2. Si $g^\omega \equiv -1$ Alors
   (a) Soit l'ordre de g est $j = 2n$ et donc $g^n \equiv -1$. Ainsi $g^{n+\omega} = 1$ et donc $\omega = n$.
   (b) Soit l'ordre de g est $j = n$ et n est impair. Alors $(g^\omega)^2 = (-1)^2 = 1$, ce qui prouve que n divise 2ω. Or n est impair donc le lemme de Gauß implique que n divise ω. Là encore $\omega = n$.

□

Ce théorème nous permet alors de conclure sur l'existence des quenines :

COROLLAIRE 2. *Soit n tel que $2n+1$ est premier. Il existe $g \in \{1, .., n\}$ tel que $\delta_{n,g}$ soit d'ordre n.*

DÉMONSTRATION. On considère la plus petite racine primitive modulo $2n+1$, $\chi(2n+1)$. Il y a deux cas :

1. Si $\chi(2n+1) \leq n$. Alors $\delta_{n,\chi(2n+1)}$ convient.
2. Sinon posons $g = \chi(2n+1)$. L'ordre j de $-g$ est soit n, soit $2n$. En effet, $g^n \equiv -1$ et donc si $(-g)^j = g^{nj+j} = 1$ alors $2n|(n+1)j$ ou encore $n|(n+1)j$ et comme n et $n+1$ sont premiers entre eux $n|j$. Ensuite, soit n est pair et donc $(-g)^n = (-1)^n g^n = g^n \neq 1$, et donc $-g$ est forcément d'ordre $2n$, soit n est impair, $(-g)^n = -(g^n) = 1$ et l'ordre de $(-g)$ est n. Dans les deux cas $\delta_{n,-\chi(2n+1)}$ convient.

□

Par exemple, la 2-dixhuitine existe, mais on peut préférer la 5-dixhuitine de rayon $\frac{18}{5} = 3.6$ qui est donnée sur la Figure 6.

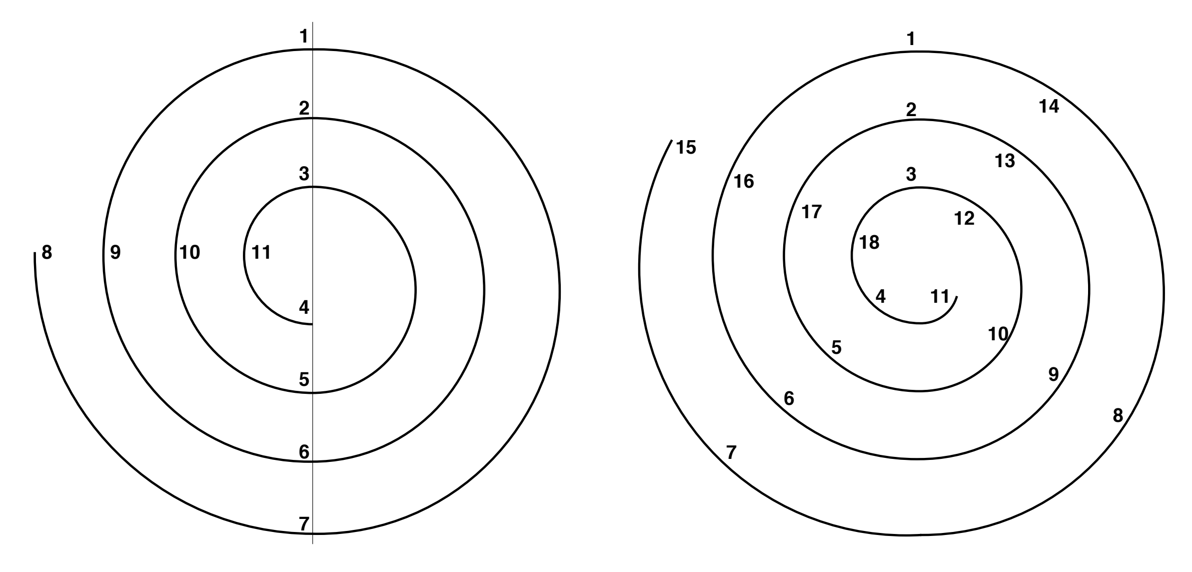


FIGURE 5. La 3-onzine

FIGURE 6. La 5-dixhuitine

En particulier, la Table 3 donne la liste des p-quenines inférieures à 1000 avec leur plus petite racine primitive.

Par ailleurs, le théorème suivant montre que l'on pourrait toujours utiliser la plus petite racine :

THÉORÈME 4 (Grosswald, 1981). *Le nombre de racines primitives modulo p dans un intervalle de taille au moins* $p^{.499}$ *est supérieur à* $c(p-1)^{.498}$ *pour* $c \leq .537$ *dès que* $\log_2(p-1) \geq 24$. *En particulier il existe alors des racines primitives modulo p inférieures à* $p^{.499}$.

Ainsi, on peut vérifier que tout premier $p \leq 16777216$ possède bien une racine primitive plus petite que $\frac{p}{2}$, (voir par exemple [Silva, 2000]). Les autres nombres premiers vérifient

$$p^{.499} \leq \frac{p-1}{2}$$

et possèdent donc une racine primitive convenable, leur plus petite racine primitive.

Néanmoins, chercher la plus petite racine primitive est plus difficile que de trouver une racine primitive quelconque, voir par exemple [Shoup, 1992 ; Murata, 1991 ; Elliott, 1997]. Le Corollaire 2 nous garantit qu'en choisissant une racine primitive au hasard, soit celle-ci soit sa négation modulo $2n+1$ sera donc plus petite que n et permettra alors la fabrication d'une n-ine.

5. LA QUÊTE DES SPININES

Il à noter qu'il est possible de fabriquer des racines primitives, au moins de manière probabiliste, avec un algorithme polynomial (donc ne nécessitant pas de factorisation de φ ni d'exploration exhaustive de l'ordre) [Dubrois, Dumas, 2006]. Les éléments

$1^\diamond$(2)	2 (2)	3 (2)	5 (2)	6 (2)	8 (3)	9 (2)	11 (2)	14 (2)	15 (3)
18 (2)	20 (6)	21 (3)	23 (2)	26 (2)	29 (2)	30 (2)	33 (2)	$35^\diamond$(2)	36 (5)
39 (2)	$41^\diamond$(2)	$44^\diamond$(3)	48 (5)	50 (2)	51 (2)	$53^\diamond$(2)	54 (6)	56 (3)	63 (3)
65 (2)	68 (3)	69 (2)	74 (2)	75 (5)	78 (5)	81 (2)	83 (2)	86 (2)	89 (2)
90 (2)	$95^\diamond$(2)	96 (5)	$98^\diamond$(2)	99 (2)	105 (2)	111 (3)	$113^\diamond$(2)	114 (6)	116 (3)
119 (2)	120 (7)	125 (3)	128 (3)	131 (2)	134 (2)	135 (2)	138 (5)	140 (3)	141 (3)
$146^\diamond$(2)	153 (5)	$155^\diamond$(2)	156 (10)	158 (2)	165 (3)	168 (10)	$173^\diamond$(2)	174 (2)	176 (3)
$179^\diamond$(2)	183 (2)	186 (2)	189 (2)	191 (2)	194 (2)	198 (5)	$200^\diamond$(3)	204 (21)	209 (2)
210 (2)	$215^\diamond$(5)	216 (5)	219 (5)	$221^\diamond$(2)	224 (3)	228 (13)	230 (2)	231 (2)	$233^\diamond$(2)
$239^\diamond$(2)	243 (2)	245 (2)	249 (5)	251 (2)	254 (2)	260 (3)	261 (2)	270 (2)	273 (2)
$278^\diamond$(2)	$281^\diamond$(2)	$284^\diamond$(3)	285 (3)	288 (5)	$293^\diamond$(2)	296 (3)	$299^\diamond$(2)	300 (7)	303 (2)
306 (2)	308 (3)	309 (2)	315 (3)	320 (3)	321 (7)	323 (2)	$326^\diamond$(2)	329 (2)	330 (2)
336 (5)	$338^\diamond$(2)	$341^\diamond$(5)	345 (3)	350 (2)	354 (2)	$359^\diamond$(2)	363 (5)	366 (6)	369 (3)
371 (2)	375 (2)	378 (2)	$380^\diamond$(6)	384 (11)	386 (2)	393 (2)	398 (2)	404 (3)	405 (3)
410 (2)	411 (2)	$413^\diamond$(2)	414 (2)	$419^\diamond$(2)	426 (2)	428 (3)	429 (2)	431 (2)	438 (2)
$440^\diamond$(3)	441 (2)	443 (2)	453 (2)	$455^\diamond$(3)	459 (5)	$464^\diamond$(3)	468 (5)	470 (2)	$473^\diamond$(2)
476 (3)	483 (2)	485 (3)	488 (3)	491 (2)	495 (2)	498 (7)	504 (11)	506 (3)	509 (2)
510 (10)	515 (2)	516 (5)	519 (2)	$524^\diamond$(3)	525 (5)	530 (2)	531 (2)	534 (6)	543 (2)
545 (2)	546 (5)	548 (3)	551 (3)	554 (2)	558 (2)	561 (2)	564 (11)	$575^\diamond$(2)	576 (5)
$581^\diamond$(3)	585 (2)	590 (7)	$593^\diamond$(2)	596 (3)	600 (11)	606 (2)	608 (3)	611 (2)	614 (2)
615 (2)	618 (2)	624 (7)	629 (2)	$638^\diamond$(2)	639 (2)	$641^\diamond$(2)	644 (6)	645 (2)	648 (10)
650 (2)	651 (2)	$653^\diamond$(2)	$659^\diamond$(2)	660 (13)	663 (3)	$680^\diamond$(3)	683 (2)	$686^\diamond$(2)	690 (2)
699 (5)	704 (3)	711 (3)	$713^\diamond$(2)	714 (6)	716 (3)	$719^\diamond$(2)	723 (2)	725 (2)	726 (2)
729 (3)	735 (5)	$740^\diamond$(3)	741 (2)	743 (2)	744 (14)	746 (2)	749 (2)	$755^\diamond$(2)	$761^\diamond$(2)
765 (2)	771 (2)	774 (2)	776 (3)	$779^\diamond$(2)	783 (2)	785 (2)	789 (3)	791 (2)	798 (11)
800 (3)	803 (2)	804 (7)	806 (3)	809 (2)	810 (2)	813 (3)	818 (2)	828 (11)	831 (2)
$833^\diamond$(2)	834 (2)	846 (2)	848 (3)	849 (3)	854 (3)	860 (3)	861 (3)	$866^\diamond$(2)	870 (2)
873 (2)	876 (7)	879 (2)	888 (5)	891 (2)	$893^\diamond$(2)	894 (6)	900 (11)	905 (3)	911 (2)
915 (3)	923 (2)	930 (2)	933 (2)	$935^\diamond$(2)	936 (10)	$938^\diamond$(2)	939 (2)	944 (3)	950 (2)
$953^\diamond$(2)	956 (3)	965 (2)	966 (5)	974 (2)	975 (2)	$986^\diamond$(2)	989 (2)	993 (2)	996 (5)
$998^\diamond$(2)	999 (3)								

TABLE 3. Les p-quenines inférieures à 1000 avec p, minimal, entre parenthèses. $^\diamond$ indique que p est d'ordre seulement n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$.

ainsi obtenus n'étant pas *prouvés* primitifs, ils sont appelés *racines primitives industrielles*. Néanmoins, aucun contre-exemple n'ayant été trouvé à [Dubrois, Dumas, 2006, algorithme 3], il semble donc possible de fabriquer de manière effective des quenines pour tout n tel que $2n+1$ est premier.

Dans [Roubaud, 1993], Jacques Roubaud se désole néanmoins que seuls les entiers n tels que $2n+1$ soit premier possèdent une permutation spirale. Il propose alors une généralisation à tous les nombres en procédant par effacement ce qui donne l'algorithme général 1 de fabrication de pseudo-quenines ou spinines.

DÉFINITION 2. *La n-*spinine*, ou n-ine puisqu'il n'y a pas d'ambiguïté est la permutation obtenue par effacements sur la $\chi(m)$-m-ine spirale avec m le plus petit entier supérieur à n tel que $2m+1$ est premier.*

Ainsi, on peut fabriquer pour tout n des permutations (ça on le savait déjà !) qui proviennent d'une permutation spirale. Afin de différencier les permutations, nous notons la 7-spinine (ou plus simplement la septine), obtenue par effacement de 8 dans la 3-octine, comme 3; 8-septine. Par opposition, la permutation qui serait obtenue par effacement des 8 et 9 dans la 2-neuvine serait notée 2; 9-septine.

Il reste à savoir comment représenter les septines sous forme de spirale. Pour cela, il faut remarquer que les nombres effacés sont successifs et plus grands que n. Ce sont donc les derniers de la spirale. En outre l'effacement va les remplacer dans la n-spinine par les entiers qui les suivent dans la m-quenine. L'idée de représentation est donc d'écrire les nombres sur les rayons classiques de la spirale en omettant les

ALGORITHME 1 Spinine [Roubaud, 1993]

Entrée Un entier $n > 0$ *quelconque.*
Sortie La spinine d'ordre n.

Trouver le plus petit $m \geq n$ tel que $2m + 1$ soit premier.
Fabriquer la $\chi(m)$-m-ine, ou si m est trop grand une m-ine quelconque en fabriquant une racine primitive industrielle.
Fabriquer l'orbite spiralique de 1 de la m-ine. Cela permet de vérifier (mais de manière non polynomiale en la taille de n) si la racine obtenue ci-dessus est bien primitive.
Dans cette orbite spiralique de 1, **effacer** tous les entiers supérieurs à n.
L'orbite ainsi obtenue est périodique de période n.

successeurs des nombres effacés. Ces successeurs sont alors écrits en fin de rayon dans l'ordre des effacements. Cela fonctionne par exemple sur la dixine obtenue à partir de la 2-onzine : $1 \quad \rightarrow \quad 6 \;\; 3 \;\; 10 \;\; 5 \;\; 9 \;\; 7 \;\; 8 \;\; 4 \;\; 2$.

Nous détaillons plutôt la fabrication de la septine par effacement de la 2-neuvine :

1. Prenons $n = 7$.
2. Choisissons $m = 9$ ($m = 8$ serait le plus petit).
3. Fabriquons [9, 1, 8, 2, 7, 3, 6, 4, 5] la 2-neuvine ...
4. Et $1 \quad \rightarrow \quad 9 \;\; 5 \;\; 7 \;\; 6 \;\; 3 \;\; 8 \;\; 4 \;\; 2$ l'orbite spiralique de 1.
5. Effaçons dans l'orbite de 1 le 8 et le 9, ils sont remplacés respectivement par 4 et 5 qui seront donc placés en fin de spirale.

La Figure 7 montre deux réalisations de la septine, les 3; 8-septine et 2; 9-septine respectivement à partir de la 3-octine et de la 2-neuvine.

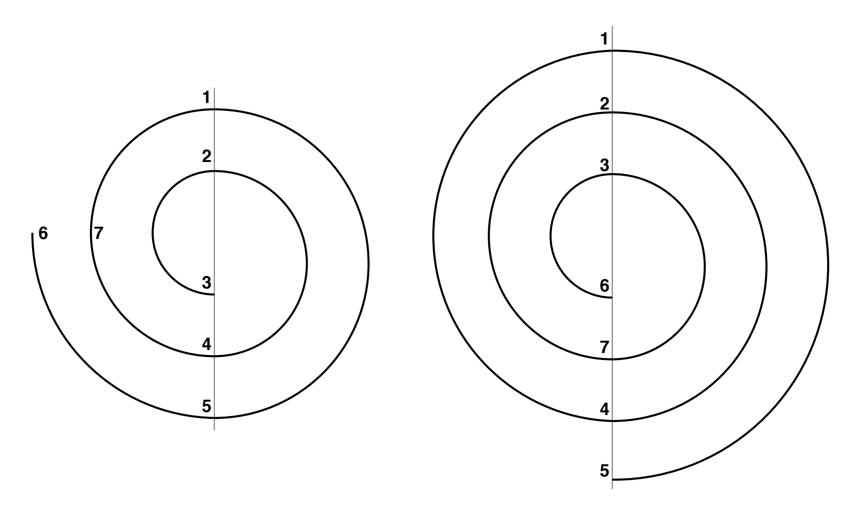


FIGURE 7. Septines, à partir de la 3-octine à gauche et de la 2-neuvine à droite.

Si la septine issue de l'octine possède bien une forme de spirale, l'effacement du 8 dans la permutation se transcrit par un simple effacement sur la spirale, on voit que celle issue de la neuvine, bien que toujours spiralique est malheureusement d'une esthétique plus discutable. En effet, il est nécessaire que les groupes "6, 7" et "4, 5" soient sur le même rayon mais ils ne s'y retrouvent pas dans un ordre croissant ...

6. PÉRECTINES

L'absence de dixine « pure » (i.e. sans effacement) a conduit Jacques Roubaud et Georges Pérec a développer une autre permutation similaire, dorénavant appelée pérecquine. En effet, Georges Pérec en a eu besoin pour le développement de son œuvre, *la vie mode d'emploi*, mais la méthode des effacements n'existait pas encore [Roubaud, 1993].

DÉFINITION 3. *Une* pérecquine *est une permutation* π_n *de l'ensemble* $\{1, 2, \ldots, n\}$ *vérifiant la condition suivante :*

$$\pi_n(x) = \begin{cases} 2x & si\ 2x \leq n \\ 2x - (n+1) & sinon \end{cases}$$

Pour ces permutations, la caractérisation est beaucoup plus simple et donne en particulier que $n + 1$ doit être premier :

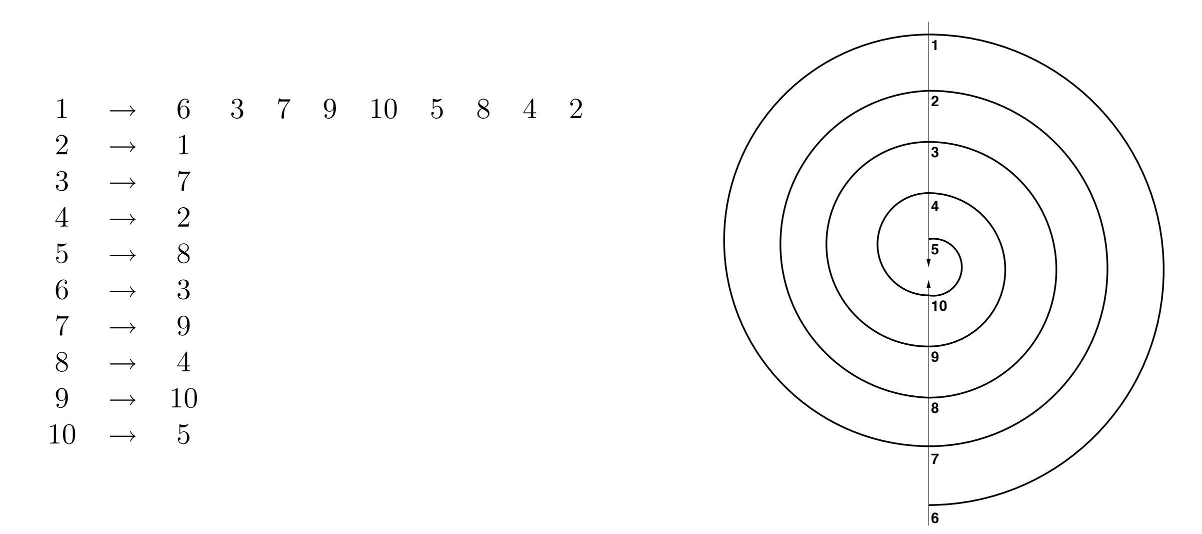
THÉORÈME 5. *La permutation* $\pi_n(x) = 2x[n + 1]$ *est d'ordre* n *si et seulement si* 2 *est d'ordre* n *modulo* $n + 1$.

DÉMONSTRATION. $\pi_n(x) = 2x \mod n + 1$ donc $\pi_n^k(x) = 2^k x \mod n + 1$. Ainsi, l'ordre spiralique de tout élément est celui de 2 dans l'anneau $\mathbb{Z}/_{n+1}\mathbb{Z}$. □

De même que pour les quenines, il est aisé de généraliser les pérecquines à tous les n tels que $n+1$ soit premier par l'utilisation d'une racine primitive. La méthode des effacements est également valable pour généraliser à tout n et nous allons voir que la représentation spirale généralisée de la Section 5. est tout à fait adaptée.

7. ORIENTATION DES RAYONS

Par analogie avec le cas des k-quenines pour $k > 2$ on donne la représentation spirale de la Figure 8 aux pérecquines : l'idée est de faire deux rayons pour chaque moitié de la permutation et de renverser le deuxième rayon par rapport aux quenines.



1	→	6	3	7	9	10	5	8	4	2
2	→	1								
3	→	7								
4	→	2								
5	→	8								
6	→	3								
7	→	9								
8	→	4								
9	→	10								
10	→	5								

FIGURE 8. Pérecquine de 10

Contrairement aux quenines, les rayons sont toujours croissants vers le centre de la spirale, même dans le cas de la généralisation à toutes les racines primitives des Figures 9 et 10. En effet, le changement d'orientation, vers l'extérieur de la spirale, correspond dans les k-quenines au changement de signe dans le calcul $\delta_n(x) = \pm k(x) \mod 2n+1$. Or les pérecquines ne présentent pas ce changement de signe et donc par conséquent elles ne présentent pas non plus le changement d'orientation des rayons.

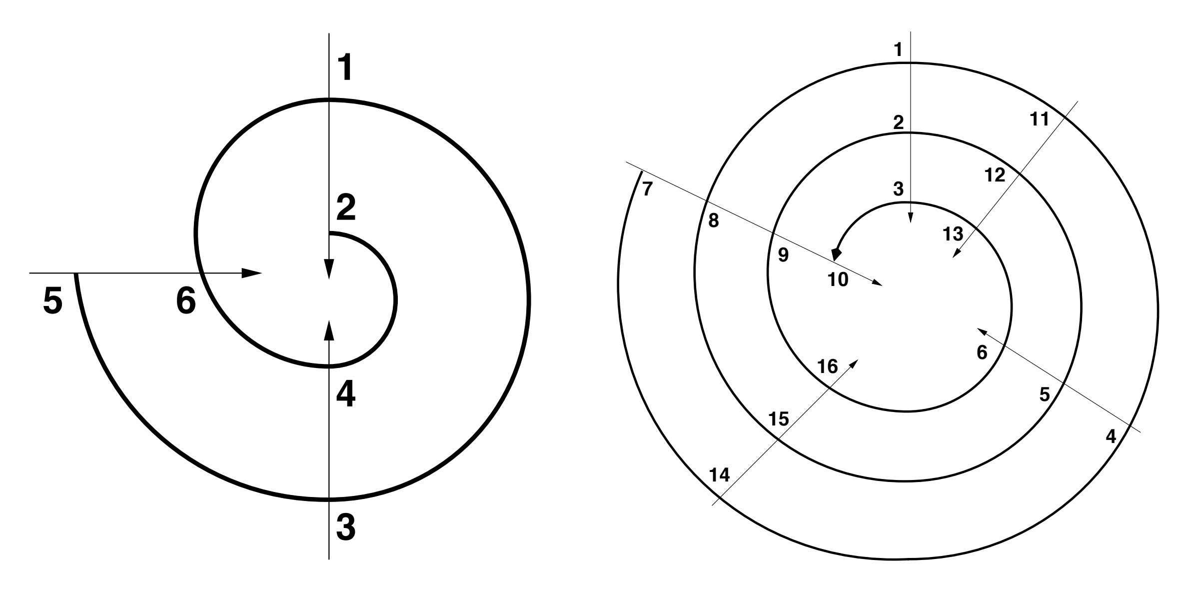


FIGURE 9. La 3-pérecquine de 6

FIGURE 10. La 5-pérecquine de 16

Cela est également le cas pour les effacements des pérecquines comme illustré sur les Figures 11 et 12.

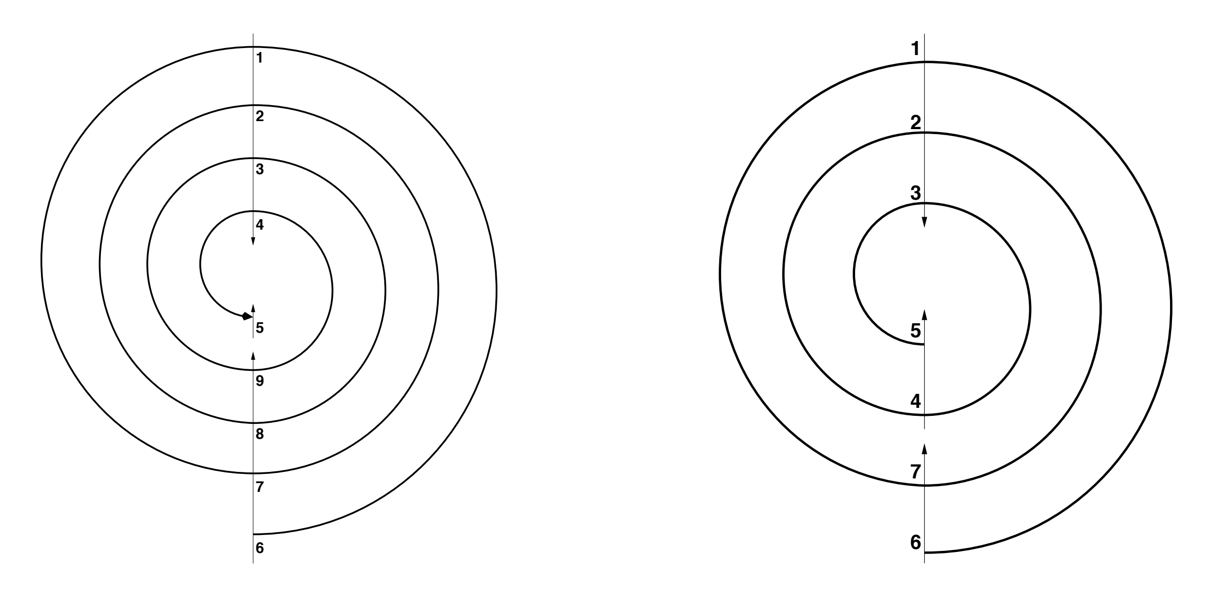


FIGURE 11. La $2, 10$-pérecquine de 9

FIGURE 12. La $2, 10$-pérecquine de 7

Dans le cas des quenines, l'alternance de l'orientation des rayons est due au changement de signe de la congruence, comme nous venons de le voir. La question qui reste posée est la détermination de cette orientation sur la représentation spirale.

En regardant les Figures 3, 4 et 5 des 3-octine, 3-neuvine et 3-onzine, on distingue deux types de $3, n$-quenines, suivant que le rayon horizontal est à gauche ou à droite.

En observant cette orientation de rayons sur plus de quenines, comme par exemple sur la Figure 13, il semble que les $3, n$-quenines de type 1 (rayon sortant à gauche) soient celles qui vérifient $n \equiv 0 \mod 3$, alors que les $3, n$-quenines de type 2 (rayon sortant à droite) vérifient $n \equiv 2 \mod 3$.

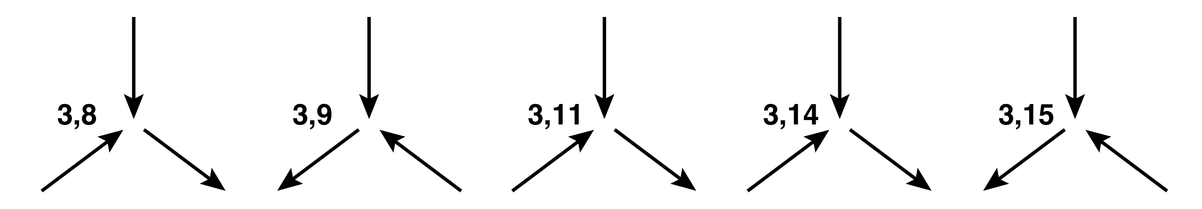


FIGURE 13. Quelques orientations de $3, n$-quenines

Une généralisation de cette conjecture permettrait alors de dessiner les g, n-quenines, comme celle de la Figure 6, sans connaissance *a priori* de la permutation générée.

BIBLIOGRAPHIE

ARNDT J., *Algorithms for programmers*, [http ://www.jjj.de/fxt/#fxtbook], [to appear 2009].

AUDIN M., « Mathématiques et littérature », *Mathématiques et Sciences humaines* 178, 2007, p. 63-86.

BACH E., SHALLIT J., *Algorithmic Number Theory : Efficient Algorithms*, Cambridge (MA), MIT press, 1996.

BRINGER M., « Sur un problème de Raymond Queneau », *Mathématiques et Sciences humaines* 27, 1969, p. 13-20.

DUBROIS J., DUMAS J.-G., "Efficient polynomial time algorithms computing industrial-strength primitive roots", *Information Processing letters* 97(2), 2006, p. 41-45.

ELLIOT P.D.T.A., MURATA L., "On the average of the least primitive root modulo p", *Journal of the London Mathematicial Society* 56(2), p. 435-454.

ESPOSITO-FARÈSE G., *Oulipian exercices* (7), 2000, [http ://www.iap.fr/users/esposito/oulipo7.html].

GROSSWALD E., "On Burgess' bound for primitive roots modulo primes and an application to γ(p)", *American Journal of Mathematics* 103(6), 1981, p. 1171-1183.

MURATA L., "On the magnitude of the least prime primitive root", *Journl of Number Theory* 37(1), 1991, p. 47-66.

OLIVEIRA E SILVA T., *Least primitive root of prime numbers*, 2000, [http ://www.ieeta.pt/~tos/p-roots.html].

ROUBAUD J., « Un problème combinatoire posé par la poésie lyrique des troubadours », *Mathématiques et Sciences humaines* 27, 1969, p. 5-12.

ROUBAUD J., « Réflexions historiques et combinatoires sur la n-ine autrement dit quenine », *La bibliothèque Oulipienne* 5(66), 2000, p. 99-124. [Contribution à la réunion 395 de l'Oulipo, le 17 septembre 1993].

SHOUP V., "Searching for primitive roots in finite fields", *Mathematics of Computation* 58(197), 1992, p. 369-380.